BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

Datenschutzim Verein -

- was ehrenamtliche Mitarbeiter wissen sollten -

KNF Kongress ´17
Nürnberg, den 26. November 2017

Thomas Kranig
Bayer. Landesamt für Datenschutzaufsicht

Agenda

1. Datenschutz – was ist das?
2. Datenschutz im Verein – wo könnte das eine Rolle spielen?
3. Handlungsempfehlungen für Vereine
4. Umgang mit Fotos, Vereinszeitung, Internet u.a.
5. Was macht die Datenschutzaufsicht?

Agenda

1. **Datenschutz – was ist das?**
2. Datenschutz im Verein – wo könnte das eine Rolle spielen?
3. Handlungsempfehlungen für Vereine
4. Umgang mit Fotos, Vereinszeitung, Internet u.a.
5. Was macht die Datenschutzaufsicht?

DATENSCHUTZ

Schutz des Einzelnen vor einer Beeinträchtigung des Persönlichkeitsrechts durch den Umgang mit seinen personenbezogene Daten

DATENSICHERHEIT (Safety)

Schutz vor ungewolltem Datenverlust (z. B. durch Plattendefekt, Feuer, ...)

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (Datenumgang) ist zunächst einmal verboten.

Zulässig sind diese Vorgänge nur, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Was sind personenbezogene Daten

„**personenbezogene Daten**“ [sind]alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels **Zuordnung** zu einer **Kennung** wie einem **Namen**, zu einer **Kennnummer**, zu **Standortdaten**, zu einer **Online-Kennung** oder zu einem oder mehreren besonderen **Merkmalen**, die Ausdruck der **physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen** oder **sozialen Identität** dieser natürlichen Person sind, identifiziert werden kann;

Welche personenbezogene Daten gibt's im Verein?

- Mitgliederverwaltung
  - Name
  - Adresse
  - Bereich
  - Bankverbindung
  - verwandt mit
  - Eintrittsdatum
  - Ehrungen
  - …
  - …
  - …

- Personalverwaltung (Übungsleiter)
  - Name
  - Adresse
  - Bereich
  - Bankverbindung
  - Steuernummer
  - Ehrungen
  - …
  - …
  - …
  - …

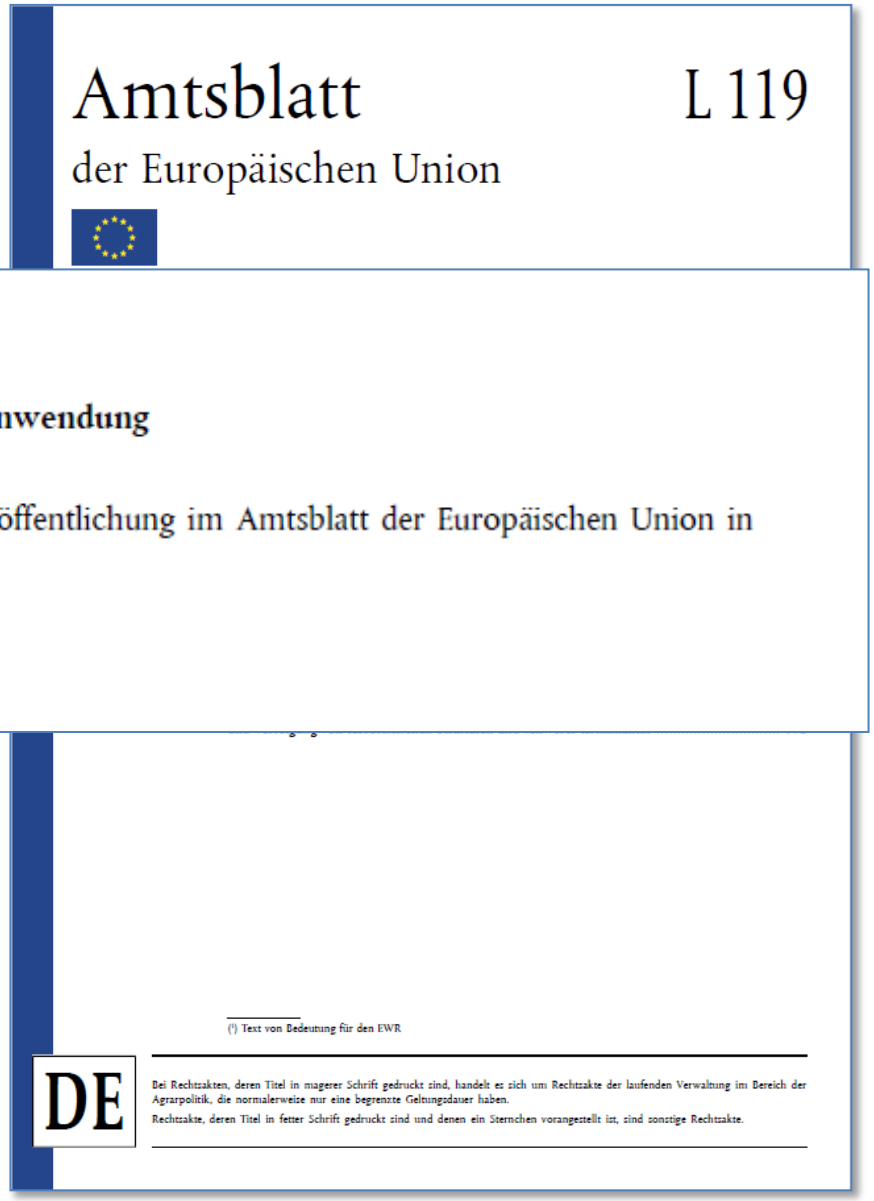
Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (Datenumgang) ist zunächst einmal verboten.

Zulässig sind diese Vorgänge nur, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Agenda

1. Datenschutz – was ist das?
2. **Datenschutz im Verein – wo könnte das eine Rolle spielen?**
3. Handlungsempfehlungen für Vereine
4. Umgang mit Fotos, Vereinszeitung, Internet u.a.
5. Was macht die Datenschutzaufsicht?

Datenschutz morgen



Amtsblatt L 119
der Europäischen Union

Artikel 99

Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.

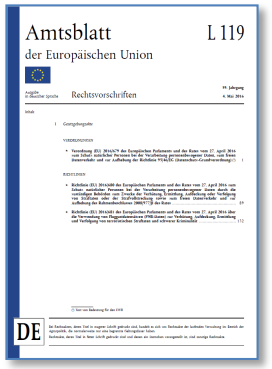
(¹) Text von Bedeutung für den EWR

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.
Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

d.h. in
nur mehr ca. 6
Monaten

Wie ist Verein von DS-GVO betroffen?


Amtsblatt L 119
der Europäischen Union
Rechtsvorschriften
DE

Artikel 2 DS-GVO
Sachlicher Anwendungsbereich

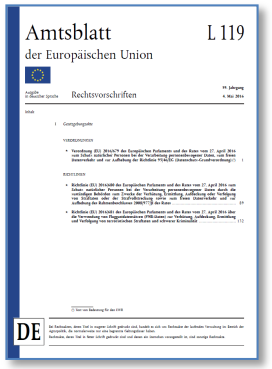
(1) Diese Verordnung gilt für die ganz oder teilweise **automatisierte** Verarbeitung personenbezogener Daten sowie für die **nichtautomatisierte Verarbeitung** personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Artikel 4 Nr. 2 DS-GVO Begriffsbestimmungen

Im Sinne der Verordnung bezeichnet :

„**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Wie ist Verein von DS-GVO betroffen?


Amtsblatt L 119
der Europäischen Union
Rechtsvorschriften
DE

Verein ist voll und ganz von der neuen Datenschutz-Grundverordnung betroffen

… wie auch bisher schon vom Bundesdatenschutzgesetz !!

Agenda

1. Datenschutz – was ist das?
2. Datenschutz im Verein – wo könnte das eine Rolle spielen?
3. **Handlungsempfehlungen für Vereine**
4. Umgang mit Fotos, Vereinszeitung, Internet u.a.
5. Was macht die Datenschutzaufsicht?

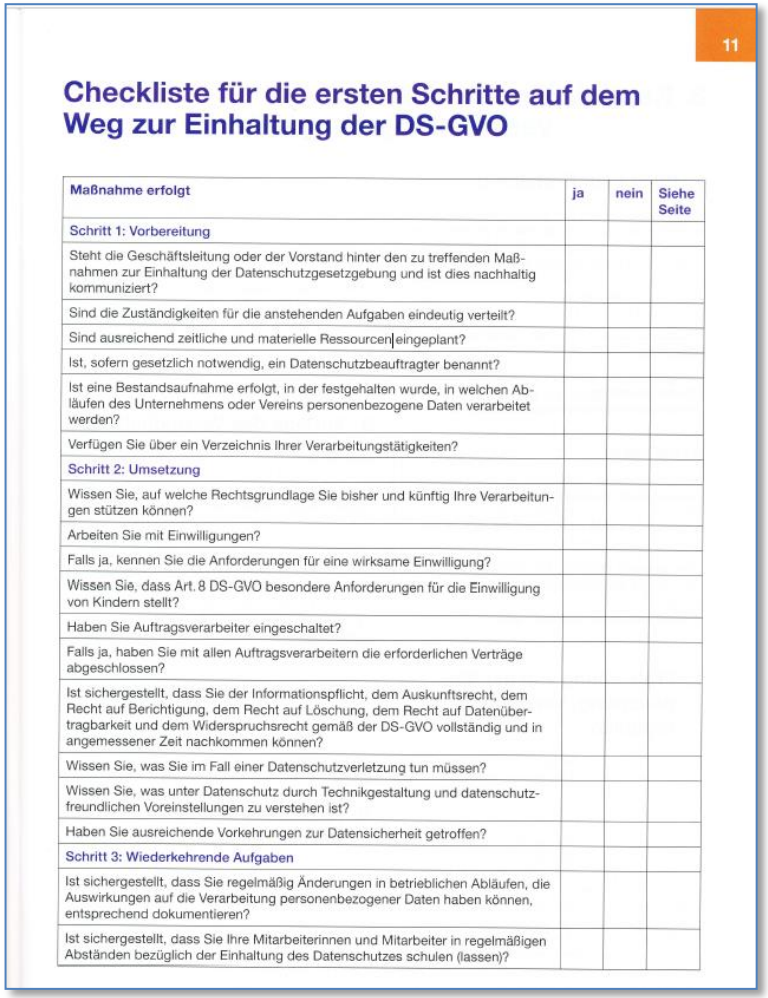
Handlungsempfehlungen für Vereine

- Übersicht verschaffen: Verzeichnis der Verarbeitungstätigkeiten
- Rechtmäßigkeit sicherstellen
- Betroffenenrechte beachten
- Auf Datenschutzverletzungen vorbereiten
- Sanktionen beachten

Handlungsempfehlungen für Vereine

- **Übersicht verschaffen: Verzeichnis der Verarbeitungstätigkeiten**
- Rechtmäßigkeit sicherstellen
- Betroffenenrechte beachten
- Auf Datenschutzverletzungen vorbereiten
- Sanktionen beachten

Handlungsempfehlungen: Übersicht verschaffen



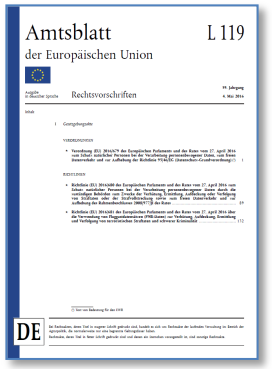
11

Checkliste für die ersten Schritte auf dem Weg zur Einhaltung der DS-GVO

Maßnahme erfolgt	ja	nein	Siehe Seite
Schritt 1: Vorbereitung			
Steht die Geschäftsleitung oder der Vorstand hinter den zu treffenden Maßnahmen zur Einhaltung der Datenschutzgesetzgebung und ist dies nachhaltig kommuniziert?			
Sind die Zuständigkeiten für die anstehenden Aufgaben eindeutig verteilt?			
Sind ausreichend zeitliche und materielle Ressourcen eingeplant?			
Ist, sofern gesetzlich notwendig, ein Datenschutzbeauftragter benannt?			
Ist eine Bestandsaufnahme erfolgt, in der festgehalten wurde, in welchen Abläufen des Unternehmens oder Vereins personenbezogene Daten verarbeitet werden?			
Verfügen Sie über ein Verzeichnis Ihrer Verarbeitungstätigkeiten?			
Schritt 2: Umsetzung			
Wissen Sie, auf welche Rechtsgrundlage Sie bisher und künftig Ihre Verarbeitungen stützen können?			
Arbeiten Sie mit Einwilligungen?			
Falls ja, kennen Sie die Anforderungen für eine wirksame Einwilligung?			
Wissen Sie, dass Art. 8 DS-GVO besondere Anforderungen für die Einwilligung von Kindern stellt?			
Haben Sie Auftragsverarbeiter eingeschaltet?			
Falls ja, haben Sie mit allen Auftragsverarbeitern die erforderlichen Verträge abgeschlossen?			
Ist sichergestellt, dass Sie der Informationspflicht, dem Auskunftsrecht, dem Recht auf Berichtigung, dem Recht auf Löschung, dem Recht auf Datenübertragbarkeit und dem Widerspruchsrecht gemäß der DS-GVO vollständig und in angemessener Zeit nachkommen können?			
Wissen Sie, was Sie im Fall einer Datenschutzverletzung tun müssen?			
Wissen Sie, was unter Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen zu verstehen ist?			
Haben Sie ausreichende Vorkehrungen zur Datensicherheit getroffen?			
Schritt 3: Wiederkehrende Aufgaben			
Ist sichergestellt, dass Sie regelmäßig Änderungen in betrieblichen Abläufen, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben können, entsprechend dokumentieren?			
Ist sichergestellt, dass Sie Ihre Mitarbeiterinnen und Mitarbeiter in regelmäßigen Abständen bezüglich der Einhaltung des Datenschutzes schulen (lassen)?			

Handlungsempfehlungen: Übersicht verschaffen

Verzeichnis von Verarbeitungstätigkeiten


Amtsblatt L 119
der Europäischen Union
Rechtsvorschriften
DE

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) **Namen** und die Kontaktdaten des Verantwortlichen …
b) **Zwecke** der Verarbeitung;
c) Beschreibung der **Kategorien betroffener Personen** und der **Kategorien personenbezogener Daten**;
d) die **Kategorien von Empfängern** …
e) gegebenenfalls Übermittlungen … Drittland …
f) wenn möglich … Fristen für die **Löschung** der verschiedenen Datenkategorien
g) wenn möglich, … Beschreibung der **technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1.

Handlungsempfehlungen für Vereine

- Übersicht verschaffen: Verzeichnis der Verarbeitungstätigkeiten
- **Rechtmäßigkeit sicherstellen**
- Betroffenenrechte beachten
- Auf Datenschutzverletzungen vorbereiten
- Sanktionen beachten

Handlungsempfehlungen: Rechtmäßigkeit sicherstellen

- **Rechtmäßigkeit (Art. 6 ff. DSGVO) bedeutet:**
  - Einwilligung liegt vor oder
  - Verarbeitung ist zur Erfüllung von Vertrag erforderlich oder
  - Verarbeitung ist zur Erfüllung rechtlicher Verpflichtung erforderlich oder
  - Verarbeitung ist zur Wahrung der ***berechtigten Interessen eines Verantwortlichen*** oder eines Dritten erforderlich, sofern nicht Interessen des Betroffenen überwiegen

Einschub: Handlungsempfehlungen: Einwilligung einholen

Eine Einwilligung (und damit die Möglichkeit auf dieser Basis Daten zu verarbeiten) **ist nur dann wirksam**,

- wenn sie freiwillig (d.h. ohne Zwang oder Druck) abgegeben wird,
- sie für einen bestimmten Fall abgegeben wird (d.h. Einwilligung zu Datenverarbeitung zu allen heute und in Zukunft relevanten Zwecken wäre unbestimmt und ungültig),
- die betroffene Person klar und verständlich informiert wurde (wer die Einwilligung haben möchte, muss klar und deutlich sagen,
- für welchen konkreten Zweck die Daten verarbeitet werden sollen),
- die betroffene Person darüber informiert wurde, dass sie die Einwilligung jederzeit widerrufen kann (ohne dass sie einen Grund angeben muss) und
- die Einwilligung schließlich durch eine eindeutig bestätigende Handlung erfolgt ist (z.B. schriftliche Erklärung, Ankreuzen einer Erklärung im Internet [sog. opt-in]; Achtung: Das „Stehenlassen“ eines bereits vorangehakten Kästchens im Internet [sog. opt-out] reicht nicht).

Handlungsempfehlungen für Vereine

- Übersicht verschaffen: Verzeichnis der Verarbeitungstätigkeiten
- Rechtmäßigkeit sicherstellen
- **Betroffenenrechte beachten**
- Auf Datenschutzverletzungen vorbereiten
- Sanktionen beachten

Handlungsempfehlungen: Betroffenenrechte beachten

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Recht auf Widerspruch
- Recht auf „nicht automatisierte Entscheidung“
- Recht auf Widerruf einer Einwilligung

Handlungsempfehlungen: Betroffenenrechte beachten

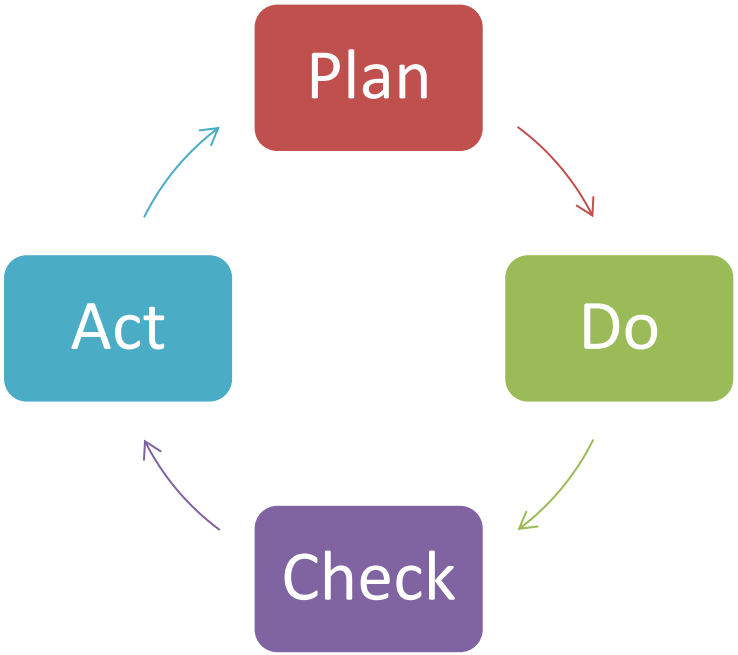
Prozessorientierter Ansatz:

Plan:
Realisierung der Betroffenenrechte und der Anforderungen zu Erfüllung

Do:
Implementierung von Verfahren zur Erfüllung der Betroffenenrechte

Check:
„Feuerwehrübung“ *(siehe „Auskunftsprojekt BayLDA“ 2016*)

Act:
Kontinuierliche Verbesserung



Handlungsempfehlungen: Betroffenenrechte beachten

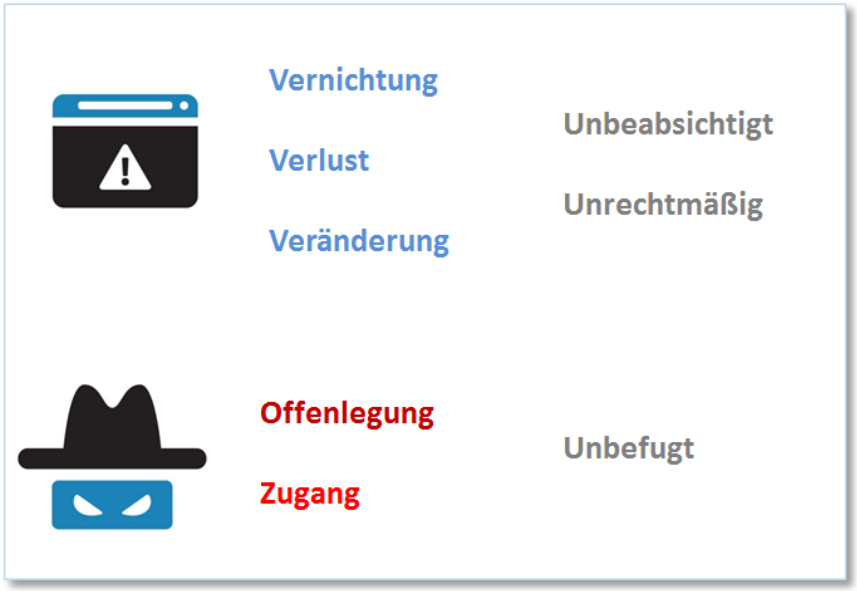
- Können Sie eine Auskunft darüber geben, welche personenbezogenen Daten Ihr Verein über bestimmte Bürger und /oder Mitglieder gespeichert hat?

- Wer ist bei Ihnen im Verein dafür verantwortlich?

Handlungsempfehlungen für Vereine

- Übersicht verschaffen: Verzeichnis der Verarbeitungstätigkeiten
- Rechtmäßigkeit sicherstellen
- Betroffenenrechte beachten
- **Auf Datenschutzverletzungen vorbereiten**
- Sanktionen beachten

Handlungsempfehlungen: Auf Datenschutzverletzung vorbereiten



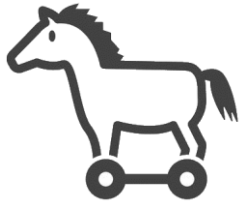
„Verletzung des Schutzes personenbezogener Daten“

ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Handlungsempfehlungen: Auf Datenschutzverletzung vorbereiten

Beispiele für Meldepflicht

- **Hacking**
- **Verlust**
- **Diebstahl**
- **Fehlversand**
- **Softwarefehler**
- **Schadcode**
- **Fehlentsorgung**
- **Vernichtung Verlust**
- **Sonstiges?**



Handlungsempfehlungen: Datenschutzverletzung erkennen

- Wer ist bei Ihnen im Verein dafür verantwortlich?
- Können Sie erkenn, wenn bei Ihnen ein Datenschutzverletzung eingetreten ist?

Handlungsempfehlungen für Vereine

- Übersicht verschaffen: Verzeichnis der Verarbeitungstätigkeiten
- Rechtmäßigkeit sicherstellen
- Betroffenenrechte beachten
- Auf Datenschutzverletzungen vorbereiten
- **Sanktionen beachten**

Handlungsempfehlungen: Sanktionen beachten

Art. 83 DS-GVO

bis **10.000.000** EUR oder 2 % Weltjahresumsatz („formelle Verstöße“)

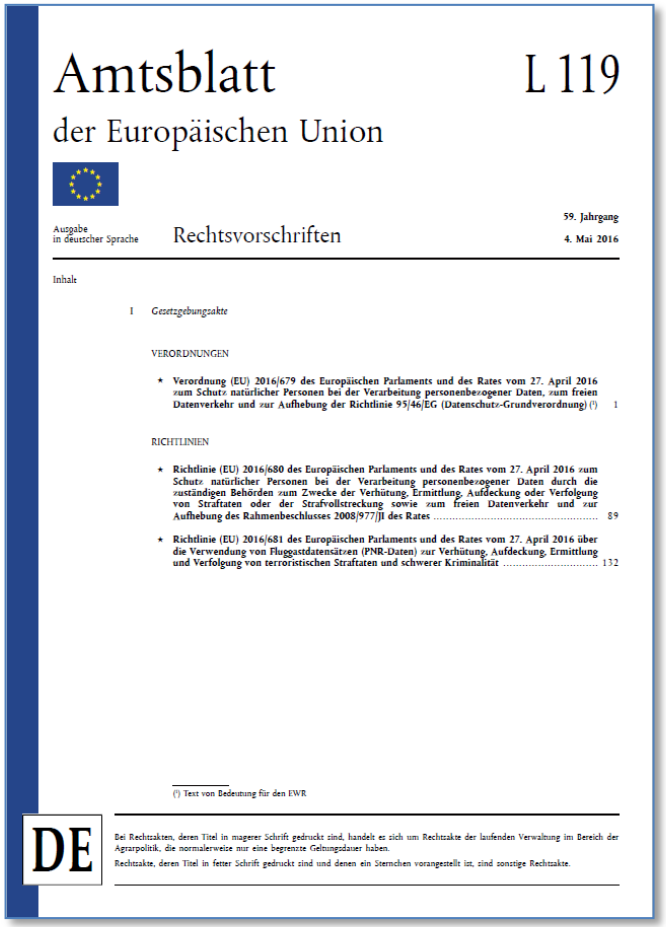
bis **20.000.000** EUR oder 4 % Weltjahresumsatz („materielle Verstöße“)

- *Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen … in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** ist. (Art. 83 Abs. 1 DS-GVO)*

Handlungsempfehlungen: Sanktionen

- **Risikoüberlegungen aktualisieren:**
  - Wie groß ist das Risiko, dass die Aufsichtsbehörde erkennt, dass bei mir/uns unzulässig mit personenbezogenen Daten umgegangen wird?
  - „Jede Aufsichtsbehörde stellt sicher … (Druck auf Aufsichtsbehörden zu sanktionieren, steigt gewaltig)

Was kann / soll man heute schon tun?



Amtsblatt L 119
der Europäischen Union

Ausgabe in deutscher Sprache — Rechtsvorschriften — 59. Jahrgang, 4. Mai 2016

Inhalt

I Gesetzgebungsakte

VERORDNUNGEN

* Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (1) 1

RICHTLINIEN

* Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates ... 89

* Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität ... 132

(1) Text von Bedeutung für den EWR

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.
Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

- bewusst machen, was kommt
- Team bilden, das das „Projekt DS-GVO“ angeht (*nicht nur Daten-schutzbeauftragte*)
- Datenumgang erfassen (**Verarbei-tungsverzeichnis**, Risikoprüfung)
- Handlungsbedarf untersuchen
- Schulungen vorbereiten
- „Feuerwehrübungen“ durchführen

Agenda

1. Datenschutz – was ist das?
2. Datenschutz im Verein – wo könnte das eine Rolle spielen?
3. Handlungsempfehlungen für Vereine
4. **Umgang mit Fotos, Vereinszeitung, Internet u.a.**
5. Was macht die Datenschutzaufsicht?

Umgang mit Bildern: Allg. Rechtsgrundlage

Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz – KUG)

§ 22

Bildnisse dürfen nur mit **Einwilligung** des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, daß er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden die Eltern des Abgebildeten.

Handlungsempfehlungen: Einwilligung einholen

Eine Einwilligung (und damit die Möglichkeit auf dieser Basis Daten zu verarbeiten) **ist nur dann wirksam**,

- wenn sie freiwillig (d.h. ohne Zwang oder Druck) abgegeben wird,
- sie für einen bestimmten Fall abgegeben wird (d.h. Einwilligung zu Datenverarbeitung zu allen heute und in Zukunft relevanten Zwecken wäre unbestimmt und ungültig),
- die betroffene Person klar und verständlich informiert wurde (wer die Einwilligung haben möchte, muss klar und deutlich sagen,
- für welchen konkreten Zweck die Daten verarbeitet werden sollen),
- die betroffene Person darüber informiert wurde, dass sie die Einwilligung jederzeit widerrufen kann (ohne dass sie einen Grund angeben muss) und
- die Einwilligung schließlich durch eine eindeutig bestätigende Handlung erfolgt ist (z.B. schriftliche Erklärung, Ankreuzen einer Erklärung im Internet [sog. opt-in]; Achtung: Das „Stehenlassen“ eines bereits vorangehakten Kästchens im Internet [sog. opt-out] reicht nicht).

Umgang mit Bildern: Allg. Rechtsgrundlage

Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz – KUG)

§ 23

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der **Zeitgeschichte**;
2. Bilder, auf denen die Personen nur als **Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
3. Bilder von **Versammlungen**, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;
4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

Handlungsempfehlungen: Einwilligung einholen

TIPP

Folgender Ratschlag völlig unjuristischer Art hat in der Praxis schon viel Ärger verhindert: Wenn Ihnen Ihr Bauchgefühl sagt, dass etwas nicht gut ist, ist es meistens auch nicht gut! Oder anders gesagt: Fragen Sie sich vor der Veröffentlichung des Fotos einer anderen Person, ob Sie es auch dann im Internet veröffentlichen würden, wenn Sie selbst auf dem Foto zu sehen wären.

Agenda

1. Datenschutz – was ist das?
2. Datenschutz im Verein – wo könnte das eine Rolle spielen?
3. Handlungsempfehlungen für Vereine
4. Umgang mit Fotos, Vereinszeitung, Internet u.a.
5. **Was macht die Datenschutzaufsicht?**

Bayerisches Landesamt für Datenschutzaufsicht

Präsident
- Leitung
- Grundsatzfragen
- Öffentlichkeitsarbeit

Geschäftsstelle

1 Referat 1
- Beschäftigten-datenschutz
- Video-überwachung

2 Referat 2
- Banken
- Auskunfteien
- Werbung
- Auftragsdaten-verarbeitung
- Kundenbindung
- Datenschutz-organisation

3 Referat 3
- Versicherungen
- Gesundheits-wesen
- Freiberufliche Tätigkeiten
- Soziale Einrichtungen

4 Referat 4
- Internet
- Telemedien
- Geodatendienste
- Apps

5 Referat 5
- Industrie
- Handel
- Bußgeldverfahren
- Internationaler Datenverkehr
- Vereine
- Vermietung und Wohneigentum

6 Referat 6
- Technischer Datenschutz
- IT-Sicherheit

Der Freistaat Bayern hat

12,7 Mio.

Einwohner

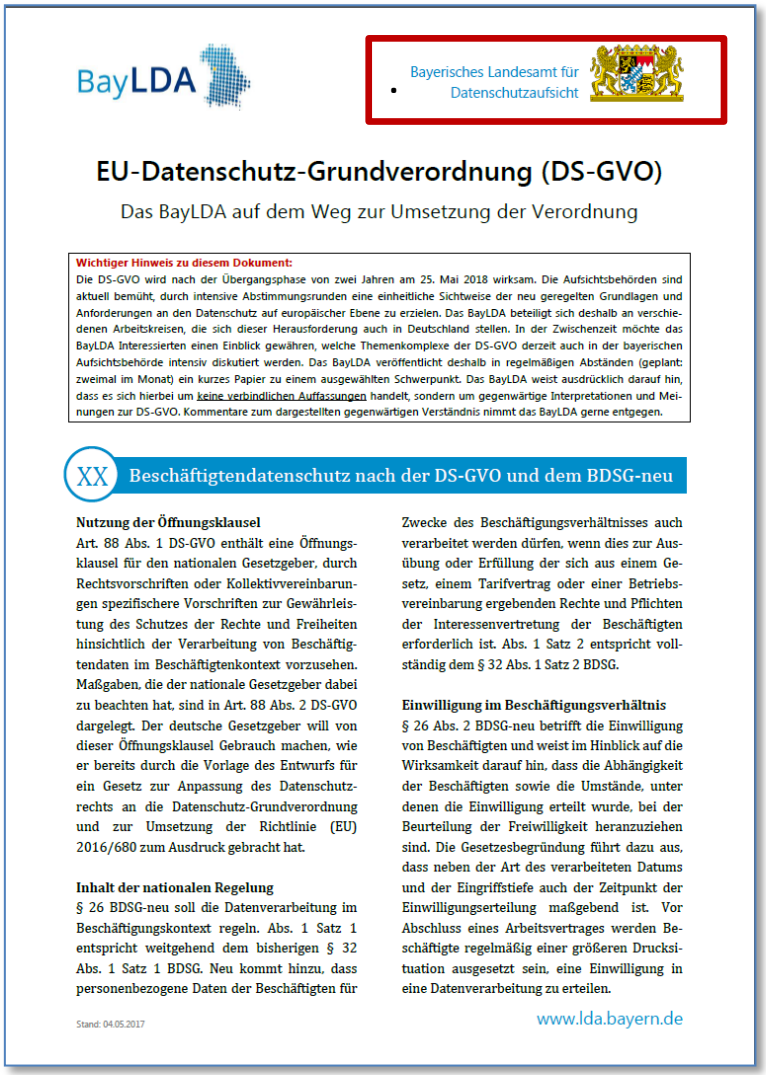
20 Planstellen

Der Freistaat Bayern hat

ca. 700.000

Unternehmen

Was macht die Datenschutzaufsicht ?



BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

EU-Datenschutz-Grundverordnung (DS-GVO)

Das BayLDA auf dem Weg zur Umsetzung der Verordnung

Wichtiger Hinweis zu diesem Dokument:
Die DS-GVO wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Die Aufsichtsbehörden sind aktuell bemüht, durch intensive Abstimmungsrunden eine einheitliche Sichtweise der neu geregelten Grundlagen und Anforderungen an den Datenschutz auf europäischer Ebene zu erzielen. Das BayLDA beteiligt sich deshalb an verschiedenen Arbeitskreisen, die sich dieser Herausforderung auch in Deutschland stellen. In der Zwischenzeit möchte das BayLDA Interessierten einen Einblick gewähren, welche Themenkomplexe der DS-GVO derzeit auch in der bayerischen Aufsichtsbehörde intensiv diskutiert werden. Das BayLDA veröffentlicht deshalb in regelmäßigen Abständen (geplant: zweimal im Monat) ein kurzes Papier zu einem ausgewählten Schwerpunkt. Das BayLDA weist ausdrücklich darauf hin, dass es sich hierbei um keine verbindlichen Auffassungen handelt, sondern um gegenwärtige Interpretationen und Meinungen zur DS-GVO. Kommentare zum dargestellten gegenwärtigen Verständnis nimmt das BayLDA gerne entgegen.

XX Beschäftigtendatenschutz nach der DS-GVO und dem BDSG-neu

Nutzung der Öffnungsklausel
Art. 88 Abs. 1 DS-GVO enthält eine Öffnungsklausel für den nationalen Gesetzgeber, durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung von Beschäftigtendaten im Beschäftigtenkontext vorzusehen. Maßgaben, die der nationale Gesetzgeber dabei zu beachten hat, sind in Art. 88 Abs. 2 DS-GVO dargelegt. Der deutsche Gesetzgeber will von dieser Öffnungsklausel Gebrauch machen, wie er bereits durch die Vorlage des Entwurfs für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 zum Ausdruck gebracht hat.

Inhalt der nationalen Regelung
§ 26 BDSG-neu soll die Datenverarbeitung im Beschäftigungskontext regeln. Abs. 1 Satz 1 entspricht weitgehend dem bisherigen § 32 Abs. 1 Satz 1 BDSG. Neu kommt hinzu, dass personenbezogene Daten der Beschäftigten für Zwecke des Beschäftigungsverhältnisses auch verarbeitet werden dürfen, wenn dies zur Ausübung oder Erfüllung der sich aus einem Gesetz, einem Tarifvertrag oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Abs. 1 Satz 2 entspricht vollständig dem § 32 Abs. 1 Satz 2 BDSG.

Einwilligung im Beschäftigungsverhältnis
§ 26 Abs. 2 BDSG-neu betrifft die Einwilligung von Beschäftigten und weist im Hinblick auf die Wirksamkeit darauf hin, dass die Abhängigkeit der Beschäftigten sowie die Umstände, unter denen die Einwilligung erteilt wurde, bei der Beurteilung der Freiwilligkeit heranzuziehen sind. Die Gesetzesbegründung führt dazu aus, dass neben der Art des verarbeiteten Datums und der Eingriffstiefe auch der Zeitpunkt der Einwilligungserteilung maßgebend ist. Vor Abschluss eines Arbeitsvertrages werden Beschäftigte regelmäßig einer größeren Drucksituation ausgesetzt sein, eine Einwilligung in eine Datenverarbeitung zu erteilen.

DSK

Kurzpapier Nr. 5
Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die DS-GVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen (insbesondere durch technische und organisatorische Maßnahmen (TOMs)) diese Risiken eingedämmt werden. Das Instrument einer Datenschutz-Folgenabschätzung (DSFA) kann hierfür systematisch eingesetzt werden.

Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr. 84, 90). Zum Begriff des Risikos, der ein zentrales Konzept der DS-GVO ist, wird es ein eigenes Kurzpapier geben.

Verarbeitungsvorgang als Ankerpunkt

Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.

Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Art. 35 Abs. 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten (-kategorien) zu gleichen Zwecken eingesetzt werden (vgl. auch ErwGr. 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen ggf. anzupassen.

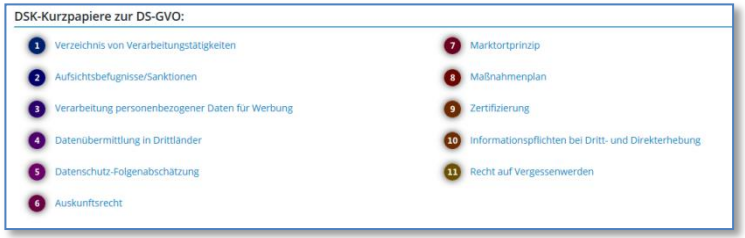
Erforderlichkeit einer DSFA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse"). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Art. 35 Abs. 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen

Was macht die Datenschutzaufsicht ?

Kurzpapiere der Datenschutzkonferenz



1. Verz. von Verarbeitungstätigkeiten
2. Aufsichtsbefugnis/Sanktionen
3. Werbung
4. Datenübermittlung in Drittländer
5. Datenschutz-Folgeabschätzung
6. Auskunftsrecht
7. Marktortprinzip
8. Maßnahmenplan
9. Zertifizierung
10. Info bei Dritt- und Direkterhebung
11. Recht auf Vergessenwerden

PLANUNG

12. Rechte und Freiheiten, Risiko
13. Privacy by Design und Default
14. Videoüberwachung (!!)
15. Besondere Kategorien pbD
16. Datenschutzbeauftragter
17. Beschäftigtendatenschutz
18. Gemeinsame Verantwortliche
19. Datenschutzverletzungen
20. Verhaltensregeln

…

Was macht die Datenschutzaufsicht ?

Noch viel wichtiger als unsere bayerischen und deutschen Kurpapiere sind aber

WORKING PAPERS

der Art. 29-Gruppe bzw. in Zukunft des Europäischen Datenschutzausschusses

Verabschiedet (und nun teilweise auch in deutsch verfügbar) sind:

- WP 242 Datenportabilität
- WP 243 Datenschutzbeauftragter
- WP 244 Federführende Aufsichtsbehörde
- WP 248 Datenschutz-Folgeabschätzung

Zur Kommentierung veröffentlicht sind:

- WP 250 Meldung von Datenschutzverletzungen
- WP 251 Profiling

In Planung sind u.a.:

- Sanktionen (Art. 83 DS-GVO)
- Dringlichkeitsverfahren (insb. Art. 66 DS-GVO)
- Beschäftigtendatenschutz

Was macht die Datenschutzaufsicht ?

Rechenschaftspflicht

Artikel 5: Grundsätze für die Vera

(1) Personenbezogene Daten müsse
a) … auf rechtmäßige Weise … („R
und Glauben, Transparenz“)
b) … für festgelegte, eindeutige und l … wecke … („Zweckbindung“)
c) … auf das notwendige Maß be … t … („Datenminimierung“)
d) … sachlich richtig … („Richti …)
e) … erforderlich … („Spei … rbegrenzung“) [und mit]
f) … angemessener Sic … rheit … („Integrität und Vertraulichkeit“)
[verarbeitet werden.]

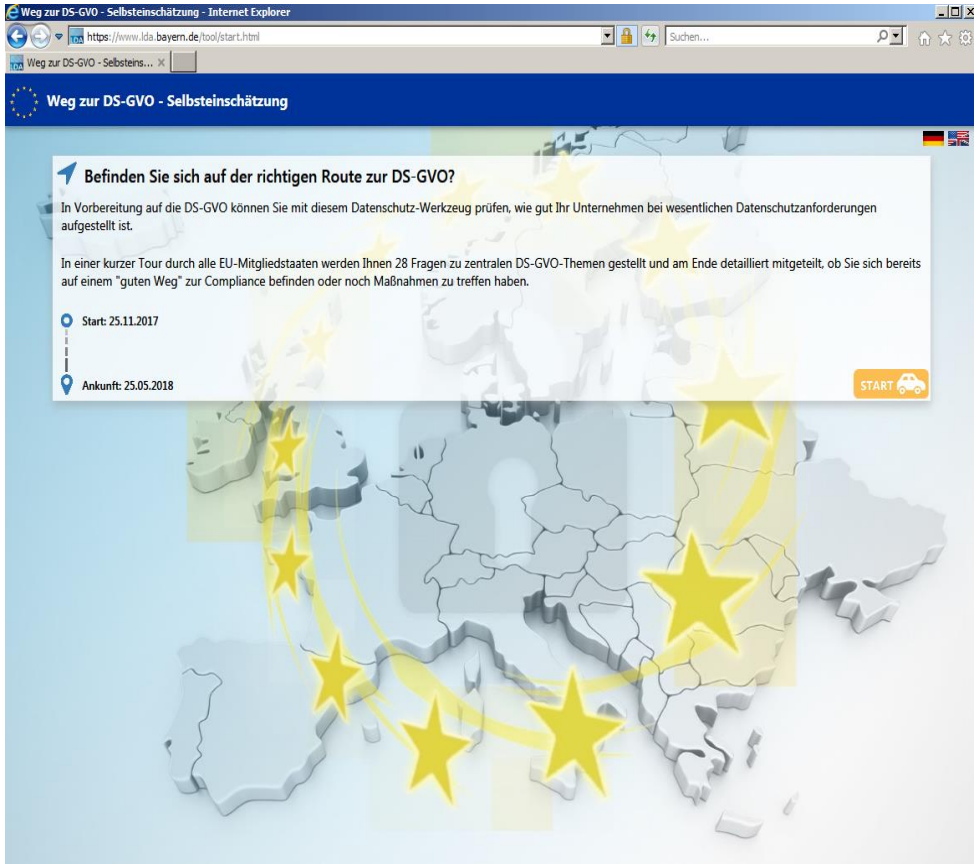
(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Wie prüfen wir:

Zeig mal !!

(„Beweislastumkehr“)

Sensibilisierung zum 25. November 2017



Rahmenbedingungen:

- 28 Fragen
- Komplett Clientbasiert
- Gewichtung der Fragen/Antworten
- Ergebnis nach Beantwortung aller Fragen
- Hinweise zu weiteren Informationen
- PDF-Generierung mit Ergebnis
- Mehrsprachig (Momentan Deutsch/Englisch)
- Einbindung in eigene Webauftritte möglich
- Online am 25.11.2017

www.lda.bayern.de

Unsere Empfehlung

Bayerisches Landesamt für
Datenschutzaufsicht

- **Datenschutz ist Chefsache** (sowohl beim Vorbeugen und Entscheiden als auch bei Sanktionen)
- **Datenschutz geht alle an** (und geht nur, wenn alle mitmachen)
- **Datenschutz gilt von Anfang an** („privacy by design“ – beziehen Sie den Datenschutz immer mit ein)
- **Schaffen Sie sich einen Überblick über Ihre aktuelle Situation** (Erstellen Sie schon heute Ihr Verarbeitungsverzeichnis nach Art. 30 DS-GVO)
- **Sprechen Sie mit Ihrer Aufsichtsbehörde** (sie kann [muss] Sie beraten – und schafft Ihnen Rechtssicherheit)
- **Haben Sie einen Plan** 

… sonst werden Sie verplant.

Nähere Infos finden Sie u.a. …

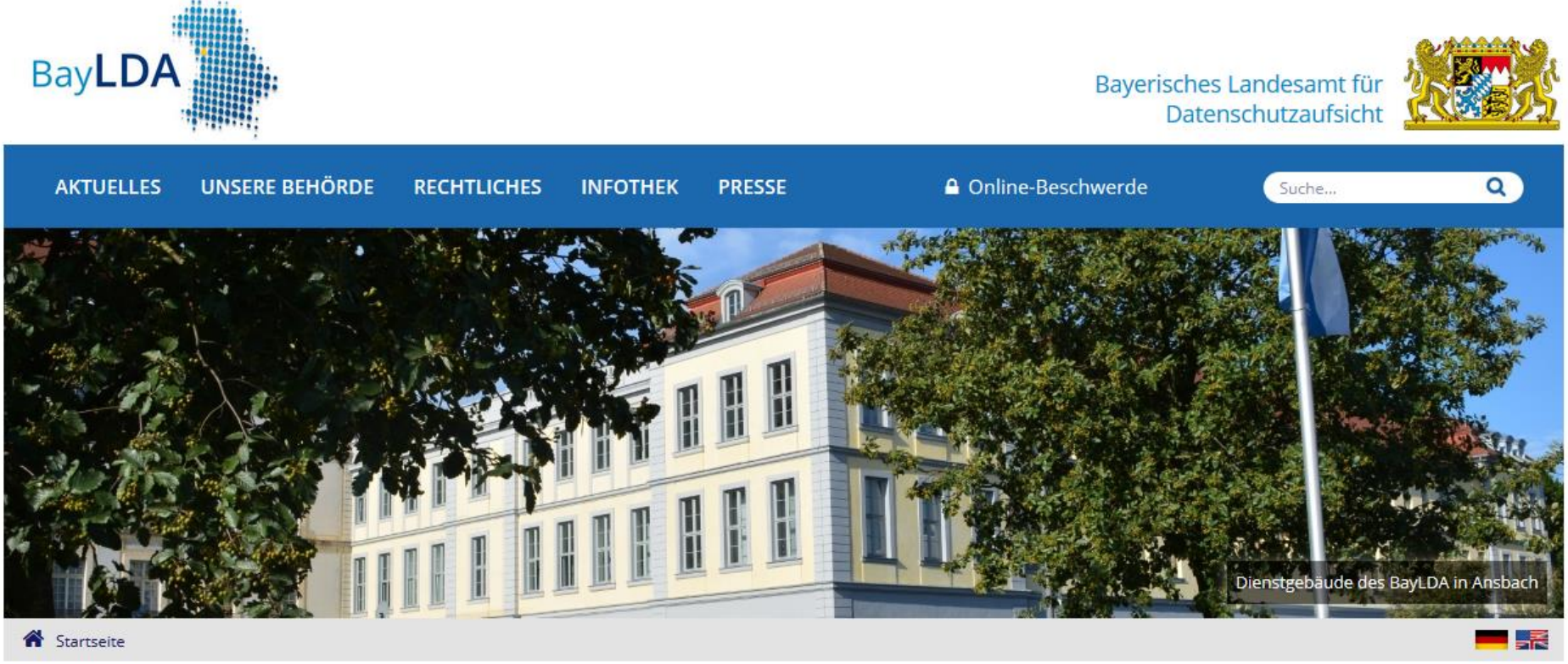
5,50 EUR

Ehmann / Kranig

Erste Hilfe zur Datenschutz-Grundverordnung

Zielgruppe:
Inhaber kleinerer Unternehmen; Vereinsvorsitzende; Datenschutzverantwortliche in kleineren Unternehmen und in Vereinen; datenschutzinteressierte Vereinsmitglieder.

Erschienen: Nov. 2017



Vielen Dank für Ihre Aufmerksamkeit

Thomas Kranig, Bayer. Landesamt für Datenschutzaufsicht

www.lda.bayern.de